

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**

06/12/2012

**06/19/2012 - UPDATED**

**SUBJECT:**

Cumulative Security Update for Internet Explorer (MS12-037)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user.

Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**June 19 - UPDATED OVERVIEW:**

*The MS-ISAC is aware of active exploitation for one of the vulnerabilities reported in MS12-037 (CVE-2012-1875). The reports are indicating that there are "limited attacks" exploiting this vulnerability. This exploit is available via a module in the Metasploit Framework.*

**SYSTEMS AFFECTED:**

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: High**

**DESCRIPTION:**

Thirteen vulnerabilities have been discovered in Microsoft Internet Explorer. Details of these vulnerabilities are as follows:

**Remote Code Execution Vulnerabilities:**

Nine remote code execution vulnerabilities have been discovered in Internet Explorer. These are memory corruption vulnerabilities that occur due to the way Internet Explorer accesses objects in memory that have not been properly deleted. These vulnerabilities may be exploited if a user visits a web page that is specifically crafted to take advantage of the vulnerabilities. Successful exploitation of any of these vulnerabilities could result in an attacker taking complete control of the system.

### Information Disclosure Vulnerabilities:

Four information disclosure vulnerabilities have also been discovered in Internet Explorer. These vulnerabilities could be exploited if an attacker convinces a user to visit a specially crafted website which would allow the attacker to access information in other domains or Internet Explorer Zones.

### RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

### REFERENCES:

#### Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms12-037>

#### Security Focus:

<http://www.securityfocus.com/bid/53866>

<http://www.securityfocus.com/bid/53867>

<http://www.securityfocus.com/bid/53868>

<http://www.securityfocus.com/bid/53869>

<http://www.securityfocus.com/bid/53870>

<http://www.securityfocus.com/bid/53871>

<http://www.securityfocus.com/bid/53841>

<http://www.securityfocus.com/bid/53842>

<http://www.securityfocus.com/bid/53843>

<http://www.securityfocus.com/bid/53844>

<http://www.securityfocus.com/bid/53845>

<http://www.securityfocus.com/bid/53847>

<http://www.securityfocus.com/bid/53848>

#### CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1523>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1858>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1872>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1873>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1874>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1875>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1876>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1877>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1878>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1879>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1880>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1881>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1882>

***June 19 – UPDATED REFERENCES***

***SANS:***

***<http://isc.sans.edu/diary.html?storyid=13495>***

***Symantec:***

***<http://www.symantec.com/connect/blogs/cve-2012-1875-exploited-wild-part-1-trojannaid>***

***Threatpost.com:***

***[http://threatpost.com/en\\_us/blogs/exploit-code-surfaces-cve-2012-1875-internet-explorer-bug-061812](http://threatpost.com/en_us/blogs/exploit-code-surfaces-cve-2012-1875-internet-explorer-bug-061812)***

***ZDNet:***

***<http://www.zdnet.com/blog/security/attack-code-published-for-critical-ie-flaw-patch-your-browser-now/12493>***